(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4150940号
(P4150940)

(45)発行日　平成20年9月17日(2008.9.17)　(24)登録日　平成20年7月11日(2008.7.11)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	540A
G09C 1/00	(2006.01)	G09C	1/00	610A
G09C 1/04	(2006.01)	G09C	1/04	
G11B 20/10	(2006.01)	G11B	20/10	H
G11B 20/12	(2006.01)	G11B	20/12	102

請求項の数 4　(全 10 頁)　最終頁に続く

(21)出願番号　特願平9-198050
(22)出願日　平成9年7月24日(1997.7.24)
(65)公開番号　特開平11-39220
(43)公開日　平成11年2月12日(1999.2.12)
審査請求日　平成15年10月28日(2003.10.28)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100082131
弁理士　稲本　義雄
(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　小林　秀和

(56)参考文献　特開平０８－０６９３５７（ＪＰ，Ａ）
特開平０７－０８５５９４（ＪＰ，Ａ）
特開平０８－２８６８４０（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】データ記録装置および方法、データ再生装置および方法、並びに伝送媒体

(57)【特許請求の範囲】

【請求項１】

セクタを最小記録単位として記録媒体に記録するデータ記録装置において、

記録すべきデータを前記セクタに対応する大きさのセクタデータに分割する分割手段と、

入力された暗号鍵に基づき、前記分割手段で分割された前記セクタデータの順序を、所定の数の前記セクタから構成されるブロックの範囲内で置換する置換手段と、

前記置換手段で置換された順序に従い、前記セクタデータを前記記録媒体に記録するとともに、前記暗号鍵も前記記録媒体に記録する記録手段と

を備え、

前記置換手段は、前記ブロックごとに異なる前記暗号鍵に基づき、前記ブロックごとに異なる規則性に従って、前記分割手段で分割された前記セクタデータの順序を、前記ブロックの範囲内で置換する

データ記録装置。

【請求項２】

セクタを最小記録単位として記録媒体に記録するデータ記録装置のデータ記録方法において、

記録すべきデータを前記セクタに対応する大きさのセクタデータに分割する分割ステップと、

入力された暗号鍵に基づき、前記分割ステップで分割された前記セクタデータの順序を

、所定の数の前記セクタから構成されるブロックの範囲内で置換する置換ステップと、
前記置換ステップで置換された順序に従い、前記セクタデータを前記記録媒体に記録するとともに、前記暗号鍵も前記記録媒体に記録する記録ステップと
を備え、
前記置換ステップは、前記ブロックごとに異なる前記暗号鍵に基づき、前記ブロックごとに異なる規則性に従って、前記分割ステップの処理で分割された前記セクタデータの順序を、前記ブロックの範囲内で置換する
データ記録方法。
【請求項３】
セクタを最小記録単位として記録媒体に記録されているデータを再生するデータ再生装置において、
前記記録媒体から暗号鍵を再生するとととともに、前記セクタに対応する大きさのセクタデータを再生する再生手段と、
再生された前記セクタデータを、ブロックを構成するセクタの数毎に区分する区分手段と、
前記区分手段で区分された、前記ブロックを構成するセクタの数と同数の前記セクタデータを、前記ブロックごとに異なる前記暗号鍵に基づいて整列する整列手段と
を備え、
前記ブロックを構成するセクタの数と同数の前記セクタデータは、前記ブロックごとに異なる前記暗号鍵に基づき、前記ブロックごとに異なる規則性に従って、その順序が前記ブロックの範囲内で置換されている
データ再生装置。
【請求項４】
セクタを最小記録単位として記録媒体に記録されているデータを再生するデータ再生装置のデータ再生方法において、
前記記録媒体から暗号鍵を再生するとととともに、前記セクタに対応する大きさのセクタデータを再生する再生ステップと、
再生された前記セクタデータを、ブロックを構成するセクタの数毎に区分する区分ステップと、
前記区分ステップで区分された、前記ブロックを構成するセクタの数と同数の前記セクタデータを、前記ブロックごとに異なる前記暗号鍵に基づいて整列する整列ステップと
を備え、
前記ブロックを構成するセクタの数と同数の前記セクタデータは、前記ブロックごとに異なる前記暗号鍵に基づき、前記ブロックごとに異なる規則性に従って、その順序が前記ブロックの範囲内で置換されている
データ再生方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、データ記録装置および方法、データ再生装置および方法、並びに伝送媒体に関し、特に、データをセクタを単位として置換することにより、データを暗号化するようにしたデータ記録装置および方法、データ再生装置および方法、並びに伝送媒体に関する。
【０００２】
【従来の技術】
最近、CD-ROMやDVD(Digital Versatile Disc)などの大容量記憶媒体の出現により、大量の音楽や映像のデジタルデータを、処理することが可能になった。これにともない、著作権保護の見地から、CD-ROM, DVDなどに記録されているオリジナルデータのコピー、改ざんを防止するセキュリティ対策が重要視されている。セキュリティ対策には、例えば、データにスクランブルをかけるなどの暗号処理が行われている。
【０００３】

【発明が解決しようとする課題】
しかしながら、従来より提案されている暗号化方法を採用すると装置の構成が複雑になるばかりでなく、コスト高になる課題があった。
【０００４】
本発明はこのような状況に鑑みてなされたものであり、データの記録再生の順番を、セクタを単位として変更することにより、簡単かつ確実に、オリジナルデータがコピー、または改ざんされることを防止するものである。
【０００５】
【課題を解決するための手段】
本発明のデータ記録装置は、記録すべきデータをセクタに対応する大きさのセクタデータに分割する分割手段と、入力された暗号鍵に基づき、分割手段で分割されたセクタデータの順序を、所定の数のセクタから構成されるブロックの範囲内で置換する置換手段と、置換手段で置換された順序に従い、セクタデータを記録媒体に記録するとともに、暗号鍵も記録媒体に記録する記録手段とを備え、置換手段は、ブロックごとに異なる暗号鍵に基づき、ブロックごとに異なる規則性に従って、分割手段で分割されたセクタデータの順序を、ブロックの範囲内で置換する。
【０００６】
本発明のデータ記録方法は、記録すべきデータをセクタに対応する大きさのセクタデータに分割する分割ステップと、入力された暗号鍵に基づき、分割ステップで分割されたセクタデータの順序を、所定の数のセクタから構成されるブロックの範囲内で置換する置換ステップと、置換ステップで置換された順序に従い、セクタデータを記録媒体に記録するとともに、暗号鍵も記録媒体に記録する記録ステップとを備え、置換ステップは、ブロックごとに異なる暗号鍵に基づき、ブロックごとに異なる規則性に従って、分割ステップの処理で分割されたセクタデータの順序を、ブロックの範囲内で置換する。
【０００８】
本発明のデータ再生装置は、記録媒体から暗号鍵を再生するとともに、セクタに対応する大きさのセクタデータを再生する再生手段と、再生されたセクタデータを、ブロックを構成するセクタの数毎に区分する区分手段と、区分手段で区分された、ブロックを構成するセクタの数と同数のセクタデータを、ブロックごとに異なる暗号鍵に基づいて整列する整列手段とを備え、ブロックを構成するセクタの数と同数のセクタデータは、ブロックごとに異なる暗号鍵に基づき、ブロックごとに異なる規則性に従って、その順序がブロックの範囲内で置換されている。
【０００９】
本発明のデータ再生方法は、記録媒体から暗号鍵を再生するとともに、セクタに対応する大きさのセクタデータを再生する再生ステップと、再生されたセクタデータを、ブロックを構成するセクタの数毎に区分する区分ステップと、区分ステップで区分された、ブロックを構成するセクタの数と同数のセクタデータを、ブロックごとに異なる暗号鍵に基づいて整列する整列ステップとを備え、ブロックを構成するセクタの数と同数のセクタデータは、ブロックごとに異なる暗号鍵に基づき、ブロックごとに異なる規則性に従って、その順序がブロックの範囲内で置換されている。
【００１１】
本発明のデータ記録装置および方法においては、記録すべきデータが、セクタに対応する大きさのセクタデータに分割され、入力された暗号鍵に基づき、分割されたセクタデータの順序が、所定の数のセクタから構成されるブロックの範囲内で置換され、置換された順序に従い、セクタデータが、記録媒体に記録されるとともに、暗号鍵も記録される。なお、置換の処理では、ブロックごとに異なる暗号鍵に基づき、ブロックごとに異なる規則性に従って、分割されたセクタデータの順序がブロックの範囲内で置換される。
【００１２】
本発明のデータ再生装置および方法においては、記録媒体から暗号鍵とセクタデータが再生され、再生されたセクタデータが、ブロックを構成するセクタ数と同数の毎に区分さ

れ、区分されたブロックを構成するセクタの数と同数のセクタデータが、ブロックごとに異なる暗号鍵に基づいて整列される。なお、ブロックを構成するセクタの数と同数のセクタデータは、ブロックごとに異なる暗号鍵に基づき、ブロックごとに異なる規則性に従って、その順序がブロックの範囲内で置換されている。

【００１３】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。

【００１４】

本発明によれば、データ記録装置が提供される。このデータ記録装置は、記録すべきデータをセクタに対応する大きさのセクタデータに分割する分割手段（例えば、図１のセクタ化回路２）と、入力された暗号鍵に基づき、分割手段で分割されたセクタデータの順序を、所定の数のセクタから構成されるブロックの範囲内で置換する置換手段（例えば、図１のセクタ順序置換回路３）と、置換手段で置換された順序に従い、セクタデータを記録媒体に記録するとともに、暗号鍵も記録媒体に記録する記録手段（例えば、図１の光ピックアップ１１）とを備え、置換手段は、ブロックごとに異なる暗号鍵に基づき、ブロックごとに異なる規則性に従って、分割手段で分割されたセクタデータの順序を、ブロックの範囲内で置換する。

【００１５】

また、本発明によれば、データ再生装置が提供される。このデータ再生装置は、記録媒体から暗号鍵を再生するとともに、セクタに対応する大きさのセクタデータを再生する再生手段（例えば、図４の光ピックアップ２１）と、再生されたセクタデータを、ブロックを構成するセクタの数毎に区分する区分手段（例えば、図４のブロック分離回路２６）と、区分手段で区分された、ブロックを構成するセクタの数と同数のセクタデータを、ブロックごとに異なる暗号鍵に基づいて整列する整列手段（例えば、図４のセクタ順序置換回路２９）とを備える。

【００１６】

但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１７】

本発明を適用したデータ記録装置の構成について、図１を参照して説明する。

【００１８】

このデータ記録装置では、インターフェイス１が、デジタルデータと暗号鍵の入力を受け付け、それぞれを、セクタ化回路２とセクタ順序置換装置３に出力するようになされている。セクタ化回路２は、入力されたデジタルデータをセクタ単位（例えば、２キロバイト）に分割し、セクタ順序置換回路３に出力するようになされている。セクタ順序置換回路３は、暗号鍵に基づいて、セクタの順序を、ブロック（例えば、１６セクタ）毎に、その範囲内で置換し、ヘッダ付加回路４に出力するようになされている。

【００１９】

ヘッダ付加回路４は、置換されたデータにセクタアドレスを含むヘッダを付加して、ECCエンコーダ５に出力するようになされている。ECCエンコーダ５は、ヘッダが付加されたデータにパリティデータをさらに付加して、ブロック化回路６に出力する。ブロック化回路６は、パリティデータが付加されたデータを所定の数（例えば、１６セクタ）毎にまとめてブロック化し、変調回路７に出力する。

【００２０】

変調回路７は、ブロック化されたデータを変調（例えば、８－１６変調）し、同期信号付加回路８に出力するようになされている。同期信号付加回路８は、変調されたデータに同期信号を付加し、記録アンプ９に出力する。記録アンプ９は、同期信号が付加されたデータを所定のレベルに増幅し、ドライバ１０に出力する。ドライバ１０は、入力されたデータに基づいて光ピックアップ１１を制御するようになされている。光ピックアップ１１は

、記録媒体１２にデータを記録するようになされている。

【００２１】

なお、図１の例の場合、ヘッダ付加回路４の後に、ECCエンコーダ５とブロック化回路６をその順番で設けているが、逆の順番、すなわち、ヘッダ付加回路４の後に、ブロック化回路６とECCエンコーダ５を順番に設置しても良い。

【００２２】

また、記録媒体１２が、DVDである場合には、１ブロックを１６セクタで構成するが、ミニディスク（MD）（商標）である場合には、１クラスタが３２セクタで構成されているので、このクラスタをブロックとして、１ブロックを３２セクタとすることができる。

【００２３】

次に、このデータ記録装置の動作について、図２のフローチャートを参照して説明する。

【００２４】

ステップＳ１において、インターフェイス１は、入力端子から、記録媒体１１に記録するデジタルデータとセクタの置換に用いられる暗号鍵の入力を受け付け、それぞれを、セクタ化回路２とセクタ順序置換回路３に出力する。ステップＳ２において、セクタ化回路２は、図３(A)に示すような、入力されたデジタルデータを、例えば、図３(B)に示すように、２キロバイトのセクタ単位に分割し、セクタ順序置換回路３に出力する。なお、図３(B)と(C)の各セクタに記述されている数字は、セクタの時系列の順序を表している。

【００２５】

ステップＳ３において、セクタ順序置換回路３は、入力されたセクタ単位のデータ（以下、セクタデータと記述する）を、インターフェイス１から入力された暗号鍵に基づいて、例えば、図３(C)に示すように、１ブロック（１６セクタ）毎に、時系列の順序を置換し、ヘッダ付加回路４に出力する。この例のように、１６セクタ毎に順序を置換した場合、セクタの順列は、１６の階乗通り存在するので、暗号鍵も、１６の階乗通り設定できる。

【００２６】

ステップＳ４において、ヘッダ付加回路４は、例えば、図３(D)に示すように、入力された各セクタデータにセクタアドレスを含むヘッダを付加し、ECCエンコーダ５に出力する。ステップＳ５において、ECCエンコーダ５は、入力されたヘッダ付セクタデータにパリティデータをさらに付加し、ブロック化回路６に出力する。ステップＳ６において、ブロック化回路６は、例えば、図３(E)に示すように、入力されたパリティデータとヘッダが付加されたセクタデータを、１６個毎にブロック化し、変調回路７に出力する。

【００２７】

ステップＳ７において、変調回路７は、ブロック化されたデータを変調し、同期信号付加回路８に出力する。ステップＳ８において、同期信号付加回路８は、変調されたブロックデータに同期信号を付加し、記録アンプ９に出力する。ステップＳ９において、記録アンプ９は、入力された同期信号付データを所定のレベルに増幅し、ドライバ１０に出力する。ドライバ１０は、入力された増幅データに基づいて光ピックアップ１１を制御し、光ピックアップ１１は、記録媒体１２にデータを記録する。

【００２８】

なお、セクタの置換の順序を示す暗号鍵は、記録媒体１２の最内周のTOC(Table of Contents)領域に記録される。

【００２９】

図１のデータ記録装置によって記録媒体１２に記録されているデータを再生するデータ再生装置の構成について、図４を参照して説明する。なお、このデータ再生装置は、図１のデータ記録装置と一体的に構成することができる。

【００３０】

このデータ再生装置では、光ピックアップ２１が、記録媒体１２のTOCとデータを読み取り、そのRF信号を２値化回路２２へ出力し、２値化回路２２は、RF信号をデジタルデータに変換し、TOCを暗号鍵抽出回路２３に、データを同期信号検出回路２４に、それぞれ出力するようになされている。

【００３１】
暗号鍵抽出回路２３は、TOCの中から暗号鍵を抽出してセクタ順序置換回路２９に出力するようになされている。同期信号検出回路２４は、入力されたデジタルデータから同期信号を検出してデジタルデータをブロックに区分し、その同期信号を取り除いて、復調回路２５に出力するようになされている。復調回路２５は、ブロックに区分されたデータを復調（変調回路７（図１）で行われた変調の復調）し、そのデータを、ブロック分離回路２６に出力する。
【００３２】
ブロック分離回路２６は、入力されたデータをブロック単位に区分してECCデコーダ２７に出力し、ECCデコーダ２７は、入力されたデータの誤りを訂正し、ヘッダ分離回路２８に出力するようになされている。ヘッダ分離回路２８は、入力されたデータからヘッダを取り除き、セクタデータをセクタ順序置換回路２９に出力する。セクタ順序置換回路２９は、入力されたセクタデータを、暗号鍵抽出回路２２から入力された暗号鍵に基づいて、元の時系列順序に置換し、インターフェイス３０に出力するようになされている。インターフェイス３０は、出力端子から再生されたデータを出力するようになされている。
【００３３】
このデータ再生装置の動作について、図５のフローチャートを参照して説明する。
【００３４】
ステップＳ２１において、光ピックアップ２１は、記録媒体１２のTOC領域を読み取り、２値化回路２２に出力する。２値化回路２２は、入力されたTOCのRF信号をデジタルデータに変換して暗号鍵抽出回路２３に出力する。ステップＳ２２において、暗号鍵抽出回路２３は、TOCから、暗号鍵を抽出し、セクタ順序置換回路２９に出力する。
【００３５】
ステップＳ２３において、光ピックアップ２１は、記録媒体１２のデータ記録領域からデータを読み取り、２値化回路２３に出力する。２値化回路２２は、入力されたRF信号をデジタルデータに変換し、同期信号検出回路２４に出力する。ステップＳ２４において、同期信号検出回路２４は、入力されたデジタルデータから同期信号を検出し、その同期信号を削除して、復調回路２５に出力する。ステップＳ２５において、復調回路２５は、入力されたデジタルデータを復調し、ブロック分離回路２６に出力する。
【００３６】
ステップＳ２６において、ブロック分離回路２６は、復調されたデータを１６セクタを１ブロックとして区分し、ECCデコーダ２７に出力する。ステップＳ２６において、ECCデコーダ２７は、入力されたデータのパリティデータを参照してデータの誤りを訂正し、ヘッダ分離回路２８に出力する。ステップＳ２８において、ヘッダ分離回路２８は、入力されたデータからヘッダを削除し、セクタデータをセクタ順序置換回路２９に出力する。
【００３７】
ステップＳ２９において、セクタ順序置換回路２９は、暗号鍵抽出回路２３から入力された暗号鍵に基づいて、１ブロック内の１６個のセクタを元の時系列順序に整列し、インターフェイス３０に出力する。ステップＳ３０において、インターフェイス３０は、出力端子から、再生されたデータを出力する。
【００３８】
なお、以上の例においては、暗号鍵を記録媒体１２のTOC領域に記録し、これを再生して用いるようにしたが、記録時と同様の暗号鍵を、外部から入力するようにしても良い。
【００３９】
記録媒体１２に記録されているデータを再生し、他の記録媒体にコピーしたとき、通常、その記録位置（セクタ）は、記録媒体１２における記録位置（セクタ）とは、異なる位置になる。その結果、コピーした暗号鍵に基づいてセクタの順序を置換しても、元の時系列の順序に戻すことができず、実質的に、データを再生することができない。従って、このように、暗号鍵の一部にセクタアドレスを用いることにより、各ブロック毎に異なる規則性でセクタの順序置換が行われ、データセキュリティが向上するだけでなく、データのコ

ピーを防ぐことができる。

【００４０】

上記各処理を行うプログラムは、磁気ディスク、CD-ROMなどの情報記録媒体よりなる伝送媒体のほか、インターネット、デジタル衛星などのネットワーク伝送媒体を介してユーザに伝送することができる。

【００４１】

【発明の効果】

以上のように、本発明によれば、データをセクタに対応する大きさに分割し、分割されたデータの順序を、ブロックの範囲内で置換し、置換したデータを、記録媒体のセクタに順番に記録するようにしたので、簡単かつ確実に、オリジナルデータがコピー、または改ざんされることを防止することができる。

【００４２】

また、本発明によれば、記録媒体からデータを再生し、再生されたデータを、所定の数のセクタ毎に区分し、区分されたデータを、所定の順番に整列させるための情報に基づいて、セクタを単位として所定の順番に整列するようにしたので、簡単かつ確実に、データを再生することができる。

【図面の簡単な説明】

【図１】本発明を適用したデータ記録装置の構成を示すブロック図である。

【図２】本発明を適用したデータ記録装置の記録処理を示すフローチャートである。

【図３】図２のステップＳ２乃至Ｓ６の処理を説明する図である。

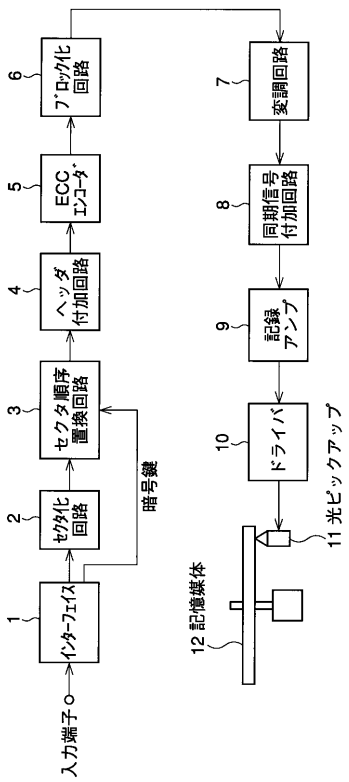
【図４】本発明を適用したデータ再生装置の構成を示すブロック図である。

【図５】本発明を適用したデータ再生装置の再生処理を示すフローチャートである。

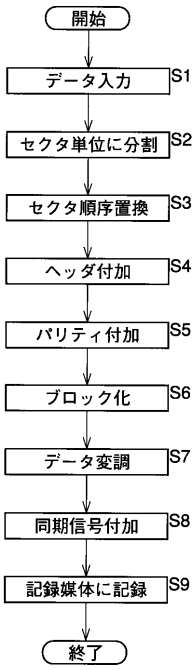
【符号の説明】

１　インターフェイス，　２　セクタ化回路，　３　セクタ順序置換回路，　４ヘッダ付加回路，　５　ECCエンコーダ，　６　ブロック化回路，　７　変調回路，　８　同期信号付加回路，　９　記録アンプ，　１０　ドライバ，　１１光ピックアップ，　１２　記録媒体，　２１　光ピックアップ，　２２　２値化回路，　２３　暗号鍵抽出回路，　２４　同期信号検出回路，　２５　復調回路，　２６　ブロック分離回路，　２７　ECCデコーダ，　２８　ヘッダ分離回路，　２９　セクタ順序置換回路，　３０　インターフェイス

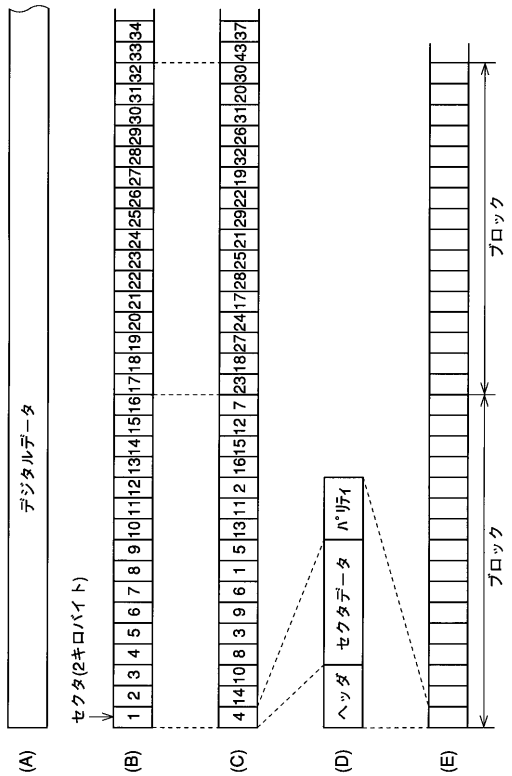
【図１】


入力端子
1 インターフェイス
2 セクタ化回路
3 セクタ順序置換回路
4 ヘッダ付加回路
5 ECCエンコーダ
6 ブロック化回路
7 変調回路
8 同期信号付加回路
9 記録アンプ
10 ドライバ
11 光ピックアップ
12 記憶媒体
暗号鍵

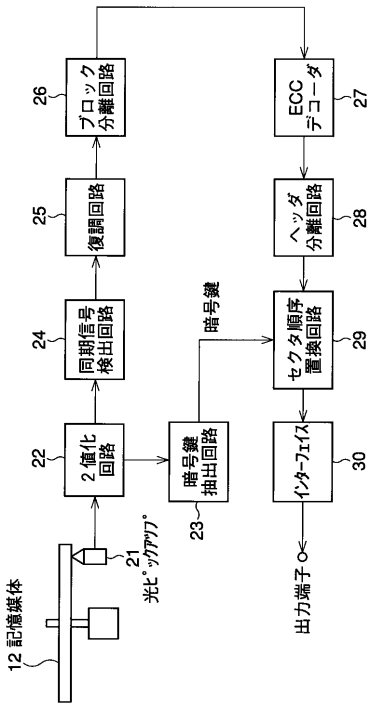
【図２】


開始
データ入力 S1
セクタ単位に分割 S2
セクタ順序置換 S3
ヘッダ付加 S4
パリティ付加 S5
ブロック化 S6
データ変調 S7
同期信号付加 S8
記録媒体に記録 S9
終了

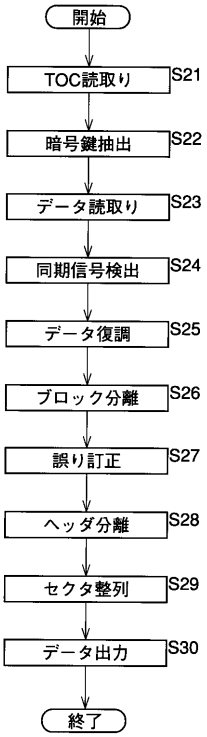
【図３】


(A)
デジタルデータ
(B)
セクタ(2キロバイト)
(C)
(D)
ヘッダ
セクタデータ
パリティ
(E)
ブロック
ブロック

【図４】


12 記憶媒体
21 光ピックアップ
22 2値化回路
23 暗号鍵抽出回路
24 同期信号検出回路
25 復調回路
26 ブロック分離回路
27 ECCデコーダ
28 ヘッダ分離回路
29 セクタ順序置換回路
30 インターフェイス
出力端子
暗号鍵

【図５】


開始
TOC読取り
S21
暗号鍵抽出
S22
データ読取り
S23
同期信号検出
S24
データ復調
S25
ブロック分離
S26
誤り訂正
S27
ヘッダ分離
S28
セクタ整列
S29
データ出力
S30
終了

フロントページの続き

(51)Int.Cl. F I

H04L 9/34 (2006.01) H04L 9/00 681

(58)調査した分野(Int.Cl., DB名)

G06F 21/24
G09C 1/00
G09C 1/04
G11B 20/10
G11B 20/12
H04L 9/34